Centrum Ekspertyzy Lokalnej

Fundacja Rozwoju Demokracji Lokalnej im. Jerzego Regulskiego

ANALIZA CELowa nr 8/2026

Cyberbezpieczeństwo małych gmin w świetle ustawy o krajowym systemie cyberbezpieczeństwa – między obowiązkami prawnymi a rzeczywistymi możliwościami organizacyjnymi

dr Kamil Czaplicki
Wydział Prawa i Administracji
Uniwersytet Kardynała Stefana Wyszyńskiego w Warszawie

1. Wstęp

Informatyzacja administracji publicznej spowodowała, że jednostki samorządu terytorialnego stały się ważnymi elementami krajowego systemu usług cyfrowych. Gminy realizują znaczną część usług publicznych, przetwarzają ogromne ilości danych oraz zapewniają mieszkańcom dostęp do coraz szerszego katalogu usług świadczonych drogą elektroniczną. Rozwój usług cyfrowych niesie niestety też zagrożenia występujące w cyberprzestrzeni.

W ciągu ostatnich lat nastąpił wyraźny wzrost liczby cyberataków wymierzonych w podmioty publiczne. Incydenty mają duży wpływ na świadczenie usług przez podmioty publiczne oraz ciągłość działania administracji publicznej. Odpowiedzią prawodawcy na wzrost liczby ataków było przyjęcie nowych regulacji prawnych, w tym w szczególności dyrektywy NIS2[1]. Jej rozwiązania zostały następnie implementowane do polskiego porządku prawnego poprzez nowelizację ustawy o krajowym systemie cyberbezpieczeństwa. Znacząco rozszerzono katalog obowiązków podmiotów objętych regulacją, wprowadzając kompleksowy model zarządzania ryzykiem cyberbezpieczeństwa, wzmacniając odpowiedzialność kierownictwa oraz akcentując konieczność budowy cyberodporności organizacji.

Celem niniejszego artykułu jest analiza wpływu nowych regulacji prawnych na funkcjonowanie małych gmin oraz próba odpowiedzi na pytanie, czy obowiązujący model regulacyjny odpowiada rzeczywistym możliwościom organizacyjnym jednostek samorządu terytorialnego.

Na potrzeby niniejszego opracowania pojęcie „małych gmin” nie odnosi się wyłącznie do liczby mieszkańców, ale jest kategorią funkcjonalną, obejmującą przede wszystkim gminy o ograniczonym potencjale kadrowym, organizacyjnym, technologicznym i finansowym. Wybór tej kategorii gmin jako przedmiotu analizy wynika z założenia, że podobne obowiązki

[1] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS2) (Dz. Urz. UE L 333 z 27.12.2022, s. 80, z późn. zm.). Stan prawny uwzględniony w opracowaniu: 24 września 2026 r.

prawne mogą powodować odmienne obciążenia organizacyjne w zależności od zasobów, jakimi dysponuje dany podmiot.

2. Cyfryzacja administracji lokalnej jako źródło nowych wyzwań w zakresie cyberodporności

W ostatnich latach jednostki samorządu terytorialnego stały się kluczowym filarem informatyzacji państwa. Realizacja większości usług publicznych odbywa się obecnie z wykorzystaniem drogi elektronicznej, a co za tym idzie – jest bezpośrednio powiązana z jakością i sprawnością funkcjonowania systemów teleinformatycznych[2]. Widoczna jest zależność pomiędzy informatyzacją jednostek samorządu terytorialnego a poziomem życia mieszkańców. Jakość życia obywateli wyraża się w udogodnieniach dotyczących zaspokajania potrzeb indywidualnych i zbiorowych w takich obszarach jak usługi społeczne (e-zdrowie, e-bezpieczeństwo, e-edukacja), ekonomiczne (e-usługi, e-praca, e-handel) i informatyczne (e-administracja, e-gospodarka)[3]. Transformacja cyfrowa nie tylko zwiększa efektywność zarządzania i realizacji usług, ale przede wszystkim zapewnia łatwiejszy i dużo bardziej przejrzysty dostęp do usług publicznych[4].

Jak wynika z raportu Komisji Europejskiej „eGovernment Benchmark 2024", średnio 88% usług administracji publicznej dla użytkowników krajowych w Europie jest dostępnych w całości online. W Polsce wskaźnik ten wynosi 84%, a więc jest zbliżony do średniej europejskiej. W raporcie z 2024 r. Polska uzyskała 69 punktów (na 100 punktów możliwych), co stanowi wzrost o 7 punktów w porównaniu z rokiem 2023[5].

Stale i dynamicznie postępująca informatyzacja administracji publicznej otwiera nowe możliwości w zakresie efektywnego zarządzania i świadczenia usług publicznych. Gminy coraz częściej i coraz chętniej wykorzystują technologie informacyjne do realizacji swoich zadań. Obserwujemy stały wzrost poziomu wykorzystania nowych technologii, powstają platformy usług lokalnych, usługi cyfrowe i strony internetowe oraz realizowane są projekty związane z cyfryzacją usług publicznych[6]. Większość gmin korzysta z rozwiązań opracowanych na poziomie centralnym i służących do realizacji zadań zleconych. Jednakże coraz częściej spotykać można jednostki rozwijające własne narzędzia, które znacząco usprawniają obsługę mieszkańców oraz budują zaufanie obywateli do instytucji publicznych. Co ważne, korzystanie z systemów lokalnych ułatwia ich integracja z Krajowym Węzłem Identyfikacji Elektronicznej (system login.gov.pl), który umożliwia bezpieczne logowanie do wielu usług administracji publicznej. Przywołany wykaz serwisów publicznych zintegrowanych z Węzłem Krajowym obejmuje 1 652 pozycje[7].

[2] B. Tubek, E-administracja i jej wpływ na współczesne społeczeństwo informacyjne, „Roczniki Administracji i Prawa" 2025, nr 2, s. 125–139.
[3] B. Kasprzyk, Aspekty funkcjonowania e-administracji dla jakości życia obywateli, „Nierówności Społeczne a Wzrost Gospodarczy" 2011, nr 23, s. 343–353.
[4] S. Kańduła, W stronę elektronicznej administracji w gminach, „Finanse Komunalne" 2023, nr 2, s. 7–26.
[5] Komisja Europejska, eGovernment Benchmark 2024, https://digital-strategy.ec.europa.eu/en/library/digital-decade-2024-egovernment-benchmark; zob. też Ministerstwo Cyfryzacji, Kluczowe wnioski z raportu eGovernment Benchmark 2024, 19 lipca 2024 r., https://www.gov.pl/web/cyfryzacja/kluczowe-wnioski-z-raportu-egovernment-bench-2024mark-2024.
[6] Szerzej: P. Drożdżewicz, E. Grudzińska, K. Hołubowicz, A. Pawluczuk, Strony internetowe urzędów gmin jako element wsparcia e-administracji w gminie, „Samorząd Terytorialny" 2014, nr 5, s. 36–47.
[7] Ministerstwo Cyfryzacji, Węzeł Krajowy – zintegrowani dostawcy usług, wykaz serwisów, platform i stron internetowych, https://archiwum_mc.bip.gov.pl/wezel-krajowy-zintegrowani-dostawcy-uslug/wezel-krajowy-zintegrowani-dostawcy-uslg.html.

Należy podkreślić, iż według przeprowadzonego przez Ministerstwo Cyfryzacji badania wdrażania nowych technologii w samorządach większość jednostek nadal wykorzystuje proste systemy informatyczne do realizacji usług publicznych. Technologie te nie są jeszcze powszechnie wykorzystywane m.in. w wyspecjalizowanych obszarach, takich jak bezpieczeństwo, gospodarka odpadami, ochrona środowiska czy smart city[8]. Jednostki samorządu terytorialnego tworzą niezwykle zróżnicowaną grupę podmiotów publicznych. Różnice dotyczą nie tylko liczby mieszkańców, powierzchni czy dochodów, ale przede wszystkim potencjału kadrowego, organizacyjnego i technologicznego. Co do zasady duże gminy miejskie radzą sobie dużo lepiej niż małe gminy wiejskie, spośród których część jeszcze kilka lat temu nie miała nawet wdrożonego ePUAP-u[9].

Informatyzacja usług publicznych ma niestety również negatywne konsekwencje. Wraz z rozwojem cyfryzacji rośnie ryzyko cyberataków prowadzących m.in. do wycieków danych czy paraliżu funkcjonowania zaatakowanego podmiotu[10]. Wraz z postępującą cyfryzacją administracji zmienił się również charakter odpowiedzialności organów gmin. Jeszcze kilkanaście lat temu głównym wyzwaniem było zapewnienie dostępności usług publicznych; obecnie istotne staje się zapewnienie odporności usług na zagrożenia występujące w cyberprzestrzeni. Odpowiedzialność za sprawne funkcjonowanie administracji obejmuje dziś bezpieczeństwo systemów teleinformatycznych, ochronę przetwarzanych danych oraz zdolność do nieprzerwanej realizacji usług publicznych pomimo wystąpienia incydentów cyberbezpieczeństwa.

Coroczny raport CERT Polska ukazuje systematyczny wzrost liczby incydentów cyberbezpieczeństwa. W 2025 r. do zespołu CERT Polska wpłynęło 658 320 zgłoszeń, na podstawie których zarejestrowano 260 783 unikalnych incydentów. W porównaniu z rokiem poprzednim był to wzrost o 152%. Najliczniejszą kategorią incydentów były oszustwa komputerowe, których odnotowano 253 238, co stanowiło 97% wszystkich zarejestrowanych incydentów. Z uwagi na temat niniejszego artykułu ważne jest zestawienie obsłużonych przez CERT Polska incydentów w podziale na sektory gospodarki. Okazuje się bowiem, iż administracja publiczna znalazła się na drugim miejscu wśród najczęściej atakowanych sektorów. CERT Polska w 2025 r. odnotował 2 801 incydentów w sektorze administracji publicznej[11]. W 2024 r. odnotowano 2 337 incydentów zakwalifikowanych do sektora administracji publicznej[12], zaś w 2023 r. takich incydentów było 2 234[13].

Statystyki pokazują, że co roku odnotowuje się kilka tysięcy incydentów w administracji publicznej; nie jest to jednak liczba zaatakowanych podmiotów. Przywołane zestawienia CERT Polska nie wyodrębniają incydentów występujących w poszczególnych kategoriach podmiotów administracji publicznej, w tym w jednostkach samorządu terytorialnego.

[8] W drodze ku doskonałości cyfrowej. Raport końcowy z badania rynku na temat gotowości wdrożenia, poziomu wiedzy i wykorzystania nowych technologii cyfrowych w jednostkach samorządu terytorialnego, Warszawa 2023, s. 11.
[9] W badaniu Edtech Hub Accelerator z 2020 r. 27 badanych gmin i powiatów zadeklarowało brak wdrożenia systemu ePUAP. Zob. Edtech Hub Accelerator, Preferencje jednostek samorządu terytorialnego w zakresie wdrożenia nowych innowacji i e-usług, 2020.
[10] Szerzej: D. Skoczylas, Cyberzagrożenia w cyberprzestrzeni. Cyberprzestępczość, cyberterroryzm i incydenty sieciowe, „Prawo w Działaniu" 2023, nr 53, s. 97–113.
[11] CERT Polska, Krajobraz bezpieczeństwa polskiego internetu. Raport roczny 2025 z działalności CERT Polska, s. 117–119, https://cert.pl/uploads/docs/Raport_CP_2025.pdf.
[12] CERT Polska, Krajobraz bezpieczeństwa polskiego internetu. Raport roczny 2024 z działalności CERT Polska, s. 91, https://cert.pl/uploads/docs/Raport_CP_2024.pdf.
[13] CERT Polska, Krajobraz bezpieczeństwa polskiego internetu. Raport roczny 2023 z działalności CERT Polska, s. 91, https://cert.pl/uploads/docs/Raport_CP_2023.pdf.

Przytoczone dane nie pozwalają zatem precyzyjnie określić skali incydentów dotyczących gmin. Potwierdzają jednak, że administracja publiczna pozostaje jednym z sektorów szczególnie narażonych na cyberzagrożenia, a zapewnienie odpowiedniego poziomu cyberodporności powinno stanowić istotny element funkcjonowania również jednostek samorządu terytorialnego.

Skutki cyberataków są dotkliwe nie tylko dla podmiotów publicznych czy też ich pracowników, ale przede wszystkim dla mieszkańców, którzy w wyniku takiego ataku mogą mieć ograniczony dostęp do usług publicznych. Z uwagi na rosnącą skalę zagrożenia kluczowe staje się zapewnienie odpowiedniego poziomu cyberodporności jednostek samorządu terytorialnego[14].

Cyberodporność jest coraz częściej używanym terminem. Zgodnie z definicją NIST cyberodporność to zdolność do przewidywania niekorzystnych warunków, obciążeń, ataków lub naruszeń dotyczących systemów wykorzystujących zasoby cybernetyczne, przeciwstawiania się im, odtwarzania zdolności działania oraz dostosowywania się do nich. Jej celem jest umożliwienie realizacji misji lub celów biznesowych zależnych od tych zasobów, także w warunkach oddziaływania zagrożeń[15]. Cyberodporność[16], w odróżnieniu od podejścia skupionego wyłącznie na zapobieganiu atakom, uwzględnia możliwość wystąpienia incydentu i potrzebę wdrożenia mechanizmów zapewniających zdolność przewidywania zagrożeń, przeciwstawiania się im, adaptacji oraz odzyskiwania zdolności działania po cyberataku[17].

W rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego[18] zdefiniowano tzw. operacyjną odporność cyfrową jako zdolność podmiotu finansowego do budowania, gwarantowania i weryfikowania swojej operacyjnej integralności i niezawodności przez zapewnianie, bezpośrednio albo pośrednio – korzystając z usług zewnętrznych dostawców usług ICT – pełnego zakresu możliwości w obszarze ICT niezbędnych do zapewnienia bezpieczeństwa sieci i systemów informatycznych, z których korzysta podmiot finansowy i które wspierają ciągłe świadczenie usług finansowych oraz ich jakość, w tym w trakcie zakłóceń[19].

Prawodawcy – zarówno europejski, jak i polski – dostrzegli rosnący problem cyberzagrożeń i przyjęli akty prawne, których celem jest podniesienie poziomu cyberbezpieczeństwa m.in. jednostek samorządu terytorialnego. Na poziomie Unii Europejskiej jest to dyrektywa NIS2,

[14] A. Gryszczyńska, Cyberbezpieczeństwo w jednostkach samorządu terytorialnego [w:] System Prawa Samorządu Terytorialnego, t. III, Samodzielność samorządu terytorialnego – granice i perspektywy, red. I. Lipowicz, Warszawa 2023.
[15] National Institute of Standards and Technology (NIST), Developing Cyber-Resilient Systems: A Systems Security Engineering Approach, NIST SP 800-160, vol. 2, rev. 1, 2021, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2r1.pdf.
[16] Szerzej: G. Szpor, The Concept of Cyber Resilience in the European Union Law, „Review of European and Comparative Law" 2026, t. 64, nr 1, s. 103–116.
[17] K. Silicki, Cyberodporność wspierana przepisami prawa UE: akt o cyberodporności (CRA) i dyrektywa NIS2 [w:] Internet. Cyberodporność, red. A. Gryszczyńska, G. Szpor, W.R. Wiewiórowski, Warszawa 2025, s. 105–117; A. Gryszczyńska, Postulaty zmian w zakresie jawności i bezpieczeństwa rejestrów publicznych [w:] Jawność i jej ograniczenia, red. G. Szpor, t. XII, Model regulacji, red. T. Bąkowski, Warszawa 2016, s. 181–197.
[18] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011 (Dz. Urz. UE L 333 z 27.12.2022, s. 1, z późn. zm.).
[19] Art. 3 pkt 1 rozporządzenia 2022/2554.

której rozwiązania implementowano do polskiego porządku prawnego poprzez nowelizację ustawy o krajowym systemie cyberbezpieczeństwa.

Budowa cyberodporności małych gmin nie jest wyłącznie problemem technicznym ani prawnym. Jest przede wszystkim wyzwaniem organizacyjnym, wymagającym odpowiedniego potencjału kadrowego, finansowego i zarządczego. Jest to zadanie szczególnie trudne dla małych gmin, które dysponują ograniczonymi zasobami organizacyjnymi i finansowymi pozwalającymi zapewnić odpowiedni poziom cyberodporności i cyberbezpieczeństwa. W praktyce duża część małych gmin funkcjonuje przy ograniczonych zasobach kadrowych i finansowych, korzystając z zewnętrznych dostawców usług IT.

3. Specyfika małych gmin jako adresatów nowych obowiązków cyberbezpieczeństwa

Obowiązki prawne wynikające z rozporządzenia RODO czy ustawy o krajowym systemie cyberbezpieczeństwa obejmują zarówno duże jednostki, jak i niewielkie gminy. Zakres stosowania obowiązków wynikających z ustawy o krajowym systemie cyberbezpieczeństwa został zróżnicowany w zależności od statusu danego podmiotu. W odniesieniu do samorządu gminnego ustawodawca zaliczył do podmiotów kluczowych urząd gminy zatrudniający na dzień 1 stycznia danego roku, w przeliczeniu na pełny wymiar czasu pracy, co najmniej 50 osób na podstawie umowy o pracę. Urząd niespełniający tego progu jest co do zasady podmiotem ważnym jako samorządowa jednostka budżetowa, o ile nie zachodzi inna podstawa uznania go za podmiot kluczowy. Z rozróżnieniem tym wiążą się uproszczenia wymagań wobec podmiotów ważnych będących podmiotami publicznymi[20].

Duże jednostki (np. Warszawa, Kraków, Gdańsk czy Wrocław) dysponują wyspecjalizowanymi komórkami odpowiedzialnymi za obsługę informatyczną, w tym również cyberbezpieczeństwo. Z drugiej strony w małych gminach często za całe utrzymanie infrastruktury teleinformatycznej odpowiada jedna osoba, czasami nawet nieposiadająca wykształcenia informatycznego. Niedobór specjalistów stanowi jedno z najpoważniejszych ograniczeń małych jednostek samorządu terytorialnego. Problem dotyczy nie tylko liczby zatrudnionych pracowników, ale również możliwości konkurowania z sektorem prywatnym pod względem wynagrodzeń. Wiele gmin zmuszonych jest korzystać z usług pojedynczych informatyków lub zewnętrznych wykonawców, którzy nie przebywają stale na terenie urzędu.

W 2025 r. przeprowadzono badania 250 najmniejszych gmin w Polsce. Autorzy badania zwrócili się, w trybie ustawy o dostępie do informacji publicznej, z pytaniem: „Czy gmina zatrudnia osobę z wykształceniem informatycznym?”. Z uzyskanych odpowiedzi wynika, że 175 gmin zatrudniało informatyka, w tym 150 – na pełny etat. W przypadku 55 gmin usługi informatyczne świadczyła firma zewnętrzna. W 12 gminach nie zatrudniano informatyka w ogóle[21].

[20] Art. 5 ust. 1 pkt 4 lit. d i ust. 2 pkt 8 oraz załącznik nr 1 (sektor podmiotów publicznych) do ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2026 r. poz. 20, z późn. zm.), dalej: ustawa o KSC. Zob. też art. 8 ust. 3, załącznik nr 4 i art. 12c tej ustawy.

Małe miejscowości borykają się również z ograniczonym budżetem, niedoborem specjalistów, a niektóre także z niewystarczającym priorytetem nadawanym problematyce cyberbezpieczeństwa przez kierownictwo jednostki. Jak słusznie zauważyła Ewelina Włoch: „Niestety, cyberbezpieczeństwo to jest coś, czym się prezydent, wójt, burmistrz nie pochwali. To nie jest medialne, tego nie widać, nikt nie widzi świetnie wyposażonej serwerowni, świetnych zabezpieczeń”[22]. Budowa cyberodporności wymaga stałych nakładów finansowych, które w przypadku wielu małych gmin pozostają trudne do sfinansowania z dochodów własnych.

Warto również zauważyć, że analizując poziom cyberodporności gmin, nie można ograniczać się wyłącznie do urzędu gminy. W praktyce zasoby kadrowe i organizacyjne odpowiedzialne za obsługę informatyczną i cyberbezpieczeństwo często wykorzystywane są również do wspierania jednostek organizacyjnych gminy, które korzystają z własnych systemów teleinformatycznych, przetwarzają dane osobowe oraz realizują zadania publiczne. Powoduje to dodatkowe obciążenie i tak już ograniczonych zasobów kadrowych i organizacyjnych małych gmin.

Uwzględniając oczywiste różnice pomiędzy jednostkami samorządu terytorialnego, należy się zastanowić, czy przyjęte zróżnicowanie obowiązków prawnych w wystarczającym stopniu odpowiada rzeczywistemu zróżnicowaniu potencjału organizacyjnego jednostek samorządu terytorialnego. Celem działania gmin nie powinno być wyłącznie formalne zapewnienie zgodności z wymogami ustawowymi, lecz stworzenie trwałego modelu zarządzania cyberbezpieczeństwem, zapewniającego odpowiedni poziom cyberodporności. Przygotowanie dokumentacji, opracowanie procedur czy też przeprowadzenie jednego szkolenia nie jest wyznacznikiem rzeczywistego poziomu cyberodporności gminy. Obecnie, w dobie wzrastających cyberzagrożeń, kluczowe znaczenie ma zdolność do praktycznego stosowania przyjętych rozwiązań, regularnego testowania procedur oraz zapewnienia ciągłości realizacji usług publicznych.

Centrum Projektów Polska Cyfrowa (CPPC) we współpracy z Naukową i Akademicką Siecią Komputerową – Państwowym Instytutem Badawczym (NASK) realizuje od 2023 r. projekt „Cyberbezpieczny Samorząd”. Celem projektu jest podniesienie poziomu cyberbezpieczeństwa JST w Polsce poprzez wzmocnienie odporności oraz zdolności do skutecznego zapobiegania i reagowania na incydenty w systemach informacyjnych[23]. Projekt skierowano do 2 807 jednostek samorządu terytorialnego, w tym 2 477 gmin. W ramach projektu przewidziano granty dla gmin na podniesienie poziomu cyberbezpieczeństwa, w szczególności zakup sprzętu i oprogramowania oraz przeprowadzenie audytów. Dodatkowo samorządy wspierane są w wykonywaniu analizy ryzyka, monitorowaniu potencjalnych zagrożeń, wykonywaniu testów penetracyjnych, wdrażaniu polityk bezpieczeństwa informacji oraz systemu zarządzania bezpieczeństwem informacji.

[21] K. Czaplicki, Zapewnienie pożądanego poziomu cyberbezpieczeństwa procesów informacyjnych realizowanych w małych i średnich gminach [w:] Cyberbezpieczeństwo – współpraca vs. konfrontacja informacyjna. Prawo – Informatyka – Zarządzanie, red. B. Szafrański, Warszawa 2025, s. 73–82.
[22] Wypowiedź Eweliny Włoch podczas CYBERSEC EXPO & FORUM 2026, przytoczona w materiale: Cyberbezpieczeństwem wójt się nie pochwali. Ale małe gminy zaczynają się budzić, Portal Samorządowy, https://www.portalsamorzadowy.pl/smart-city/cyberbezpieczenstwem-wojt-sie-nie-pochwali-ale-male-gminy-zaczynaja-sie-budzic,665039.html.
[23] Ministerstwo Cyfryzacji, Cyberbezpieczny Samorząd – zakończenie naboru, https://www.gov.pl/web/baza-wiedzy/cyberbezpieczny-samorzad--zakonczenie-naboru; Centrum Projektów Polska Cyfrowa, Cyberbezpieczny Samorząd, https://www.gov.pl/web/cppc/cyberbezpieczny-samorzad.

Elementem projektu jest również tworzenie zespołów reagowania na incydenty oraz edukowanie pracowników z zakresu cyberbezpieczeństwa.

Projekt jest realizowany w ramach programu Fundusze Europejskie na Rozwój Cyfrowy 2021–2027, a w Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej zapowiedziano kontynuację projektu. Jak można przeczytać w Strategii: „Kontynuowany będzie program Cyberbezpieczny Samorząd obejmujący szkolenia i zakupy niezbędnego sprzętu i oprogramowania. Rząd będzie wspierać JST w budowie i rozbudowie samorządowych struktur odpowiedzialnych za cyberbezpieczeństwo tych jednostek, co jest szczególnie istotne biorąc pod uwagę ograniczone zasoby poszczególnych JST”[24].

Co więcej, rząd zobowiązał się do budowy Lokalnych Centrów Cyberbezpieczeństwa, działających jako centra usług wspólnych w obszarze IT, które będą minimalizowały skutki braków kadrowych i niedoboru specjalistów z obszaru cyberbezpieczeństwa w małych jednostkach samorządu terytorialnego. Zakłada się, że Lokalne Centra Cyberbezpieczeństwa zapewnią wysoki poziom cyberbezpieczeństwa dla wielu instytucji działających na szczeblu lokalnym i regionalnym[25]. Realizacji tego kierunku służy nabór na tworzenie Lokalnych Centrów Cyberbezpieczeństwa, uruchomiony przez CPPC 31 lipca 2026 r.[26].

Pozytywnie należy ocenić zarówno kontynuację projektu „Cyberbezpieczny Samorząd”, jak i działania na rzecz budowy Lokalnych Centrów Cyberbezpieczeństwa. Cyberbezpieczeństwo jest procesem wymagającym ciągłego doskonalenia, regularnych szkoleń pracowników i stałego dostosowywania się do zmieniających się zagrożeń. Współpraca samorządów w ramach Lokalnych Centrów Cyberbezpieczeństwa stanowi wyraz współdzielenia kompetencji oraz zasobów i może się przyczynić do lepszego ich zagospodarowania.

4. Obowiązki wynikające z dyrektywy NIS2 i ustawy o krajowym systemie cyberbezpieczeństwa

Dynamiczny rozwój cyberzagrożeń spowodował, że regulacje dotyczące cyberbezpieczeństwa przestały mieć wyłącznie charakter techniczny, lecz stały się jednym z podstawowych elementów systemu bezpieczeństwa państwa. Obowiązki JST wynikają obecnie z wielu aktów prawa krajowego i unijnego, które wzajemnie się uzupełniają, tworząc wielowarstwowy model ochrony systemów teleinformatycznych. Regulacje dotyczące cyberbezpieczeństwa są rozproszone w licznych aktach prawnych.

Obowiązki związane z zapewnieniem bezpieczeństwa informacji i systemów teleinformatycznych w jednostkach samorządu terytorialnego wynikają z wielu aktów prawa krajowego i unijnego. Do najważniejszych regulacji tworzących otoczenie prawne funkcjonowania JST w tym obszarze należą w szczególności:

[24] Uchwała nr 92 Rady Ministrów z dnia 10 marca 2026 r. w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej (M.P. poz. 309), załącznik, pkt 5.2, https://eli.gov.pl/api/acts/MP/2026/309/text/O/M20260309.pdf.
[25] Tamże, załącznik, pkt 5.2.
[26] Centrum Projektów Polska Cyfrowa, Działanie 4.1 – Cyberbezpieczeństwo, trzeci nabór, FERC.04.01-IP.01-003/26 (Lokalne Centra Cyberbezpieczeństwa), nabór rozpoczęty 31 lipca 2026 r., https://www.gov.pl/web/cppc/FERC0401IP0100326.

1. rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 4.05.2016, s. 1 z późn. zm.).
2. rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (Dz. Urz. UE L 257 z 28.08.2014, s. 73 z późn. zm.).
3. rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie) (Dz. Urz. UE L 151 z 7.06.2019, s. 15 z późn. zm.).
4. ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2026 r. poz. 20 z późn. zm.).
5. ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz. U. z 2025 r. poz. 1703 z późn. zm.).
6. ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (t.j. Dz. U. z 2024 r. poz. 1725 z późn. zm.).
7. rozporządzenie Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2024 r. poz. 773).

Zakres obowiązków wynikających z wymienionych regulacji jest zróżnicowany, a ich znaczenie dla funkcjonowania gmin nie jest jednakowe. Z punktu widzenia przedmiotu niniejszego opracowania szczególne znaczenie ma ustawa o krajowym systemie cyberbezpieczeństwa, która wprost określa obowiązki podmiotów objętych krajowym systemem cyberbezpieczeństwa w zakresie zarządzania ryzykiem, stosowania środków technicznych i organizacyjnych, obsługi i zgłaszania incydentów, zapewnienia ciągłości działania oraz odpowiedzialności kierownictwa. Z tego względu dalsza analiza zostanie skoncentrowana przede wszystkim na obowiązkach wynikających z tej ustawy oraz na ocenie możliwości ich realizacji przez małe gminy.

Przepisy dotyczące cyberbezpieczeństwa są rozproszone, a także często zmieniane[27], co utrudnia ich skuteczne wdrażanie, szczególnie w małych miejscowościach, w których cały proces zapewnienia cyberbezpieczeństwa spoczywa na jednej osobie, która – co równie ważne – ma często także inne obowiązki służbowe. W odniesieniu do dynamiki wdrażania przepisów z zakresu cyberbezpieczeństwa G. Szpor wskazywała, iż „pogodzenie wymagań szybkiej adaptacji przepisów do nowych potrzeb z zasadami stabilności, spójności i przejrzystości prawa wymaga przełamania separacji i poprawy koordynacji równoległych procesów legislacyjnych”[28]. Rozproszenie regulacji powoduje, że zapewnienie zgodności z wymogami prawnymi wymaga jednoczesnego stosowania przepisów należących do różnych gałęzi prawa. Kierownictwo gmin, szczególnie tych małych, musi uwzględniać jednocześnie przepisy dotyczące cyberbezpieczeństwa, ochrony danych osobowych,

[27] Szerzej: Jawność i jej ograniczenia, t. I, Idee i pojęcia, red. G. Szpor, C.H. Beck, Warszawa 2017.
[28] G. Szpor, The Evolution of Cybersecurity Regulation in the European Union Law and Its Implementation in Poland, „Review of European and Comparative Law” 2021, nr 3, s. 234.

informatyzacji działalności podmiotów realizujących zadania publiczne czy też usług zaufania. Tak szeroki katalog regulacji stanowi istotne wyzwanie organizacyjne, zwłaszcza dla jednostek borykających się z brakami kadrowymi[29].

Na potrzeby niniejszego artykułu postanowiono skupić się głównie na ustawie o krajowym systemie cyberbezpieczeństwa, której przepisy wprost odnoszą się do cyberbezpieczeństwa.

Dyrektywa NIS2 stanowi obecnie podstawowy akt prawny Unii Europejskiej, adresowany do władz państw członkowskich i regulujący kwestie cyberbezpieczeństwa podmiotów świadczących usługi o kluczowym znaczeniu dla funkcjonowania zarówno państwa, jak i gospodarki. Dyrektywa została przyjęta w celu zwiększenia odporności cyfrowej oraz zapewnienia wysokiego i jednolitego poziomu bezpieczeństwa na obszarze całej Unii Europejskiej. Bez wątpienia eskalacja cyberzagrożeń istotnie wpływa na aktualną politykę Unii Europejskiej. W ciągu ostatnich kilku lat w centrum zainteresowania Unii Europejskiej znalazły się zagadnienia dotyczące skutecznej ochrony cyberprzestrzeni przed działaniami dezinformacyjnymi, cyberprzestępczością czy cyberwojną[30]. Dyrektywa wyznacza nowe standardy zarządzania cyberbezpieczeństwem w Unii Europejskiej, uznając je za jeden z podstawowych elementów bezpieczeństwa państwa. Należy podzielić pogląd, iż „znaczenie bezpieczeństwa informacyjnego i cyberbezpieczeństwa dla wielu państw jest priorytetem w utrzymaniu prawidłowego poziomu bezpieczeństwa narodowego”[31].

Dyrektywa ma zlikwidować rozbieżności w wymogach cyberbezpieczeństwa i w realizacji środków cyberbezpieczeństwa w różnych państwach członkowskich. W tym celu wprowadziła minimalne standardy ram regulacyjnych i mechanizmy skutecznej współpracy między właściwymi organami w każdym państwie członkowskim. Ustawodawca uaktualnił listę sektorów i działań objętych obowiązkami w zakresie cyberbezpieczeństwa oraz wskazał środki naprawcze i sankcje zapewniające ich wykonanie[32]. Obecna dyrektywa 2022/2555 zastąpiła wcześniejszą dyrektywę 2016/1148, wprowadzając znacznie szerszy zakres podmiotowy i przedmiotowy, a także zaostrzając obowiązki w zakresie zarządzania ryzykiem cyberbezpieczeństwa. W dyrektywie położono szczególny nacisk na odpowiedzialność kadry zarządzającej, która została zobowiązana do aktywnego uczestnictwa w procesie zarządzania cyberbezpieczeństwem oraz ponoszenia odpowiedzialności za niewłaściwe wykonywanie obowiązków.

Dyrektywa nakłada na podmioty zobowiązane, w tym również podmioty publiczne, obowiązek wdrożenia środków zarządzania ryzykiem w cyberbezpieczeństwie. Obejmują one m.in. prowadzenie analizy ryzyka, stosowanie odpowiednich środków technicznych i organizacyjnych, zarządzanie incydentami, zapewnienie ciągłości działania, bezpieczeństwo łańcucha dostaw, stosowanie mechanizmów uwierzytelnienia oraz regularne szkolenia personelu. Położono również duży nacisk na zgłaszanie incydentów do właściwych organów[33]. Warto podkreślić, iż dyrektywa NIS2 wprowadziła odejście od modelu koncentrującego się przede wszystkim na reagowaniu na incydenty na rzecz modelu zarządzania ryzykiem oraz budowy odporności organizacyjnej.

[29] Szerzej: W.Z. Dziomdziora, Cyberbezpieczeństwo w samorządzie terytorialnym. Praktyczny przewodnik, Warszawa 2021.
[30] D. Skoczylas, Wzmocnienie zdolności Unii Europejskiej w zakresie cyberbezpieczeństwa – cybersolidarność w kontekście cyberzagrożeń, „Europejski Przegląd Sądowy” 2024, nr 12, s. 39–44.
[31] S. Woszek, Cyberbezpieczeństwo państw w XXI wieku na przykładzie Rzeczypospolitej Polskiej, „Przegląd Bezpieczeństwa Wewnętrznego” 2022, nr 27(14), s. 206.
[32] R. Bujalski, Nowe środki w zakresie cyberbezpieczeństwa (dyrektywa NIS2), LEX/el. 2023.
[33] Szerzej: Dyrektywa NIS2. Komentarz, red. M. Jakubik, R.T. Prabucki, Gdańsk 2026.

Dyrektywa 2022/2555 została implementowana do krajowego porządku prawnego ustawą z dnia 23 stycznia 2026 r. o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (Dz. U. poz. 252), która weszła w życie 3 kwietnia 2026 r. Implementacja nastąpiła zatem z opóźnieniem względem terminu 17 października 2024 r. określonego w art. 41 dyrektywy NIS2. We wrześniu 2026 r. trwa okres dostosowawczy: podmioty spełniające przesłanki uznania za kluczowe lub ważne w dniu wejścia w życie nowelizacji mają, co do zasady, wdrożyć obowiązki rozdziału 3 do 3 kwietnia 2027 r. Termin na złożenie wniosku o wpis do wykazu przypada zasadniczo 3 października 2026 r.[34].

Ustawa o krajowym systemie cyberbezpieczeństwa tworzy podstawy prawno-instytucjonalne dla cyberbezpieczeństwa na poziomie krajowym. Celem regulacji jest zapewnienie odpowiedniego poziomu bezpieczeństwa sieci i systemów teleinformatycznych wykorzystywanych przez podmioty realizujące zadania o istotnym znaczeniu dla bezpieczeństwa państwa, gospodarki oraz społeczeństwa[35]. W ustawie określono organizację krajowego systemu cyberbezpieczeństwa, zadania i kompetencje organów właściwych oraz obowiązki podmiotów objętych jej zakresem, w tym również podmiotów publicznych. Ustawa wprowadza ramy prawne służące zapobieganiu, wykrywaniu i reagowaniu na incydenty cyberbezpieczeństwa. Ustawa o KSC stała się obecnie jednym z najważniejszych instrumentów prawnych służących budowie odporności cyfrowej państwa[36].

Ustawa o krajowym systemie cyberbezpieczeństwa nałożyła na podmioty publiczne wiele obowiązków. Do głównych obszarów obowiązków adresowanych do jednostek samorządu terytorialnego możemy zaliczyć zarządzanie bezpieczeństwem informacji z uwzględnieniem ryzyka, obsługę incydentów oraz zapewnienie ciągłości działania. Ich szczegółowy zakres zależy jednak od statusu podmiotu.

Szczególne znaczenie dla funkcjonowania podmiotów publicznych ma art. 8, który nakłada obowiązek wdrożenia kompleksowego systemu zarządzania bezpieczeństwem informacji, obejmującego zarówno aspekty techniczne, jak i organizacyjne. System ten staje się elementem bieżącego zarządzania jednostką. System zarządzania bezpieczeństwem informacji powinien obejmować cały cykl funkcjonowania systemów informacyjnych, zaczynając od identyfikacji i analizy ryzyka, poprzez wdrożenie odpowiednich zabezpieczeń, monitorowanie zagrożeń, zarządzanie incydentami, a kończąc na zapewnieniu ciągłości działania oraz odtworzeniu funkcjonowania po wystąpieniu incydentu.

W odniesieniu do podmiotu ważnego będącego podmiotem publicznym art. 8 ust. 3 wyłącza jednak stosowanie ust. 1 i odsyła do uproszczonych wymagań określonych w załączniku nr 4. Obejmują one m.in. inwentaryzację zasobów, kontrolę dostępu, wykonywanie i testowanie odseparowanych kopii zapasowych, przygotowanie i testowanie procedur na wypadek awarii lub incydentu, cyberhigienę i szkolenia oraz regularny przegląd systemu[37].

[34] Art. 41 ust. 1 dyrektywy NIS2; ustawa z dnia 23 stycznia 2026 r. o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (Dz. U. poz. 252), w szczególności art. 33 ust. 1; Ministerstwo Cyfryzacji, Nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa (KSC) – obowiązki podmiotów kluczowych i ważnych, https://www.gov.pl/web/cyfryzacja/nowelizacja-ustawy-o-krajowym-systemie-cyberbezpieczenstwa-ksc---obowiazki-podmiotow-kluczowych-i-waznych.

[35] Szerzej: G. Szpor [w:] Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz, red. K. Czaplicki, A. Gryszczyńska, G. Szpor, Warszawa 2019.

[36] Szerzej: C. Banasiński, M. Rojszczak, J.M. Chmielewski, W. Hydzik, J. Łuczak, W. Nowak, K. Waćkowski, Krajowy system cyberbezpieczeństwa [w:] Cyberbezpieczeństwo, Warszawa 2020.

Warto zauważyć, iż art. 8 ustawy o KSC rozwija podejście znane z § 19 rozporządzenia w sprawie Krajowych Ram Interoperacyjności[38], który również określał obowiązek opracowania i stosowania systemu zarządzania bezpieczeństwem informacji zapewniającego poufność, dostępność i integralność danych przetwarzanych przez podmiot publiczny. Art. 8 ust. 1 ustawy o KSC szczegółowo wskazuje elementy, które muszą znaleźć się w systemie zarządzania bezpieczeństwem informacji, wprowadza obowiązek uwzględnienia bezpieczeństwa łańcucha dostaw, akcentuje ciągłość monitorowania systemu, wymaga wdrożenia planów ciągłości działania i odtworzenia po awarii, a także kładzie szczególny nacisk na cyberhigienę pracowników. W przypadku publicznych podmiotów ważnych należy natomiast stosować wymagania załącznika nr 4, bez automatycznego przenoszenia na nie całego katalogu obowiązków z art. 8 ust. 1. Wdrożenie systemu zarządzania bezpieczeństwem informacji nie może być utożsamiane wyłącznie z przygotowaniem dokumentacji wymaganej przez przepisy prawa, lecz ma być mechanizmem ciągłego doskonalenia bezpieczeństwa informacji, który powinien funkcjonować jako istotny element codziennego zarządzania jednostką.

Ustawodawca w większym niż dotychczas stopniu zaakcentował odpowiedzialność kierownictwa za wdrażanie systemów cyberbezpieczeństwa. Wprost wskazano w art. 8c, iż odpowiedzialność za wykonywanie obowiązków wskazanych w tym przepisie ponosi kierownik podmiotu kluczowego lub ważnego, w tym podmiotu publicznego. Co istotne, odpowiedzialność kierownika występuje również wówczas, gdy niektóre z obowiązków albo wszystkie obowiązki zostały powierzone innej osobie za jej zgodą. Oznacza to, że wójt, burmistrz lub prezydent miasta nie może ograniczyć swojej roli do delegowania obowiązków informatykowi lub zewnętrznemu dostawcy, gdyż to na kierowniku spoczywa obowiązek zapewnienia odpowiednich zasobów oraz odpowiedzialność za realizację obowiązków. Rozwiązanie to oznacza odejście od utrwalonego przez wiele lat modelu, zgodnie z którym kwestie związane z bezpieczeństwem teleinformatycznym były zadaniem informatyków. Obecnie odpowiedzialność spoczywa na najwyższym szczeblu zarządzania.

Kierownicy podmiotów publicznych objętych ustawą na mocy jej art. 8d odpowiadają za organizację i nadzór nad systemem zarządzania bezpieczeństwem informacji. Przepis nakłada na kierownictwo obowiązek podejmowania decyzji dotyczących przygotowania, wdrażania, stosowania oraz doskonalenia systemu zarządzania bezpieczeństwem informacji. Kierownictwo odpowiada za zapewnienie odpowiednich środków finansowych niezbędnych do realizacji obowiązków w zakresie cyberbezpieczeństwa, właściwy podział zadań pomiędzy pracowników oraz nadzór nad ich wykonywaniem. Na szczególną uwagę zasługuje obowiązek budowania świadomości pracowników poprzez zapewnienie stałych szkoleń i znajomości obowiązujących procedur wewnątrz organizacji.

Ustawodawca, dostrzegając rolę i znaczenie kierownictwa organizacji w procesie zapewniania cyberodporności, w art. 8e ustawy o KSC zobowiązał kierownika podmiotu kluczowego lub ważnego oraz osobę, której powierzono obowiązki kierownika w zakresie cyberbezpieczeństwa, do odbywania szkolenia raz w roku kalendarzowym. Nie jest to tożsame z objęciem tym konkretnym obowiązkiem wszystkich pracowników

[37] Art. 8 ust. 1 i 3 oraz załącznik nr 4 do ustawy o KSC. Dla podmiotów ważnych będących podmiotami publicznymi ustawodawca przewidział odrębny katalog wymagań wobec systemu zarządzania bezpieczeństwem informacji.
[38] § 19 rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. poz. 773).

odpowiedzialnych za cyberbezpieczeństwo. Celem rozwiązania jest zapewnienie, aby osoby odpowiedzialne za zarządzanie posiadały wiedzę umożliwiającą prawidłowe wykonywanie obowiązków. Udział w szkoleniu musi być udokumentowany; przepis nie wymaga określonej formy imiennego certyfikatu. Zakres szkolenia obejmuje wykonywanie obowiązków wskazanych w art. 8e ust. 2, w szczególności związanych z systemem zarządzania bezpieczeństwem informacji, zadaniami kierownictwa, obsługą i zgłaszaniem incydentów, stosowaniem środków technicznych i organizacyjnych oraz współpracą z właściwymi podmiotami systemu[39]. W ustawie o KSC, podobnie jak w rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2019/881, podkreśla się szczególne znaczenie zachowań użytkowników, wskazując na potrzebę rozwijania tzw. cyberhigieny, czyli prostych, codziennych działań ograniczających ryzyko cyberataków[40].

Ustawa o KSC, w szczególności art. 8 ust. 1, kładzie duży nacisk na bezpieczeństwo łańcucha dostaw. W przypadku publicznych podmiotów ważnych ocenę wymagań należy opierać na załączniku nr 4; nie oznacza to jednak, że zależność od dostawców traci znaczenie organizacyjne. Małe gminy w dużym stopniu opierają funkcjonowanie systemów na usługach świadczonych przez podmioty zewnętrzne. Bezpieczeństwo gmin uzależnione jest tym samym od bezpieczeństwa dostawców usług IT.

Istotnym obowiązkiem wynikającym z ustawy o krajowym systemie cyberbezpieczeństwa jest zgłaszanie incydentów. Przez incydent rozumie się zdarzenie, które ma lub może mieć niekorzystny wpływ na bezpieczeństwo systemów informacyjnych. Ustawodawca wyróżnia m.in. incydenty krytyczne, poważne oraz incydenty w cyberbezpieczeństwie na dużą skalę. Obsługa incydentu to, zgodnie z definicją ustawową, czynności umożliwiające jego wykrywanie, rejestrowanie, analizowanie, klasyfikowanie, priorytetyzację, podejmowanie działań naprawczych i ograniczenie skutków. W ogólnym modelu z art. 11 ust. 1 pkt 4–4c wczesne ostrzeżenie o incydencie poważnym przekazuje się niezwłocznie, nie później niż w ciągu 24 godzin od jego wykrycia, a zgłoszenie incydentu – niezwłocznie, nie później niż w ciągu 72 godzin od wykrycia. Zgłoszenie zawiera aktualizację informacji i wstępną ocenę zdarzenia, nie zaś ostateczny, pełny opis. Sprawozdanie końcowe należy przekazać najpóźniej w ciągu miesiąca od zgłoszenia incydentu. Jeżeli jego obsługa nadal trwa, w tym terminie składa się sprawozdanie z postępu obsługi, a sprawozdanie końcowe – najpóźniej w ciągu miesiąca od jej zakończenia. Na żądanie właściwego CSIRT-u składa się także sprawozdanie okresowe[41].

Dla małych urzędów zasadnicze znaczenie ma jednak art. 12c: podmiot ważny będący podmiotem publicznym nie przekazuje wczesnego ostrzeżenia ani sprawozdań okresowego, z postępu obsługi i końcowego. Nadal ciąży na nim obowiązek zgłoszenia incydentu poważnego niezwłocznie, nie później niż w ciągu 72 godzin od wykrycia, a także pozostałe obowiązki z art. 11 i 12, z uwzględnieniem tego wyłączenia[42].

Docelowym adresatem zgłoszeń jest właściwy CSIRT sektorowy. Przepisy przejściowe przewidują jednak, że do czasu ogłoszenia osiągnięcia przez niego zdolności operacyjnej informacje kieruje się do właściwego krajowego CSIRT-u. Dla urzędów gmin jest nim co do zasady CSIRT NASK, z zastrzeżeniem szczególnych reguł właściwości. Od dnia następującego po publikacji stosownego komunikatu zgłoszenia należy przekazywać do CSIRT-

[39] Art. 8e ust. 1–3 ustawy o KSC; obowiązek udokumentowania uczestnictwa wynika z ust. 3.
[40] Szerzej: Internet. Hacking, red. A. Gryszczyńska, G. Szpor, W.R. Wiewiórowski, Warszawa 2023.
[41] Art. 11 ust. 1 pkt 4–4c oraz art. 12, 12a i 12b ustawy o KSC.
[42] Art. 12c ustawy o KSC.

u sektorowego. Właściwość adresata trzeba zatem ustalać z uwzględnieniem aktualnego etapu organizacji systemu[43].

Ustawa o krajowym systemie cyberbezpieczeństwa duży nacisk kładzie na zachowanie ciągłości działania. Idea ciągłości działania znajduje wyraz w normie ISO 22301:2019, w której pojęcie to rozumiane jest jako zdolność organizacji do utrzymania realizacji kluczowych procesów na akceptowalnym poziomie po wystąpieniu zakłócenia. Jest to zatem proces zapewnienia, iż kluczowe funkcje mogą być kontynuowane podczas krytycznych zdarzeń i po nich, takich jak awarie systemów, katastrofy naturalne czy ataki cybernetyczne[44]. Głównym celem zasady ciągłości działania jest zapewnienie możliwie szybkiego wznowienia działalności oraz ograniczenie negatywnych skutków incydentów.

Koncepcja ta pozostaje w ścisłym związku z przepisami ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, której celem jest zapewnienie sprawnego funkcjonowania administracji w sytuacji zagrożenia. Zarządzanie kryzysowe obejmuje działania polegające na zapobieganiu sytuacjom kryzysowym, przygotowaniu do przejmowania nad nimi kontroli, reagowaniu w przypadku ich wystąpienia, usuwaniu skutków takich sytuacji oraz odtwarzaniu zasobów i infrastruktury krytycznej. Coraz częściej źródłem takich zdarzeń są incydenty cyberbezpieczeństwa, które mogą prowadzić do zakłócenia realizacji zadań publicznych przez jednostki samorządu terytorialnego. Zapewnienie ciągłości działania systemów oraz procesów realizowanych przez gminę stanowi istotny element budowania jej odporności na sytuacje kryzysowe[45].

System zarządzania ciągłością działania przyjmuje postać udokumentowanego zestawu procedur i mechanizmów reagowania na zdarzenia kryzysowe, takie jak pożar, powódź, awaria techniczna, strajk, zmiana otoczenia prawnego czy cyberatak. Obejmuje on zarówno działania prewencyjne, zmierzające do ograniczenia ryzyka wystąpienia zakłóceń, jak i rozwiązania umożliwiające sprawne odtworzenie zdolności operacyjnej po ich zaistnieniu. Zgodnie z normą ISO 22301 system ten powinien podlegać ciągłemu doskonaleniu i być rozwijany adekwatnie do zmian zachodzących w organizacji. W konsekwencji zarządzanie ciągłością działania należy uznać za kluczowy element zapewnienia trwałości funkcjonowania organizacji w warunkach zakłóceń[46].

Warto również zauważyć, że chociaż ustawa o KSC nie nakłada na radę gminy bezpośrednio obowiązków w zakresie cyberbezpieczeństwa, to realizacja zadań wynikających z tej ustawy pozostaje w znacznym stopniu uzależniona od decyzji organu stanowiącego, w szczególności w zakresie uchwalenia budżetu, zapewnienia odpowiednich środków finansowych oraz sprawowania kontroli nad działalnością organu wykonawczego. W konsekwencji skuteczne zapewnienie cyberbezpieczeństwa gminy wymaga współpracy zarówno organu wykonawczego, jak i stanowiącego.

Interesującym przykładem implementacji dyrektywy NIS2 jest Republika Czeska, w której zakres regulacji różnicuje się zależnie od rodzaju gminy. Gminy o rozszerzonych

[43] Art. 26 ust. 6 pkt 1 lit. aa oraz art. 27 ustawy o KSC; art. 42 ust. 2 i art. 44 ust. 1–2 ustawy z dnia 23 stycznia 2026 r. o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (Dz. U. poz. 252).
[44] M. Górnisiewicz, Skuteczne zarządzanie ciągłością działania [w:] Zarządzanie ryzykiem bankowym, red. M. Iwanicz-Drozdowska, Warszawa 2024.
[45] Art. 2 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (t.j. Dz. U. z 2026 r. poz. 574 z późn. zm.). Szerzej na temat odporności JST: I. Lipowicz, Odporność samorządu terytorialnego, „Samorząd Terytorialny" 2025, nr 4, s. 32–42.
[46] L. Kępa, Bezpieczeństwo danych osobowych. Podejście oparte na ryzyku, C.H. Beck, Warszawa 2019, Legalis.

kompetencjach (*obce s rozšířenou působností*) objęto reżimem niższych obowiązków, natomiast pozostałe gminy – I i II typu – mają odpowiednio zabezpieczać administrowane przez siebie systemy informacyjne administracji publicznej, bez nakładania na nie pozostałych obowiązków nowej ustawy. Rozwiązanie to ilustruje znaczenie proporcjonalności regulacji do zakresu zadań i potencjału jednostki. W modelu o niższych obowiązkach istotne są m.in. szkolenia pracowników, wykonywanie kopii zapasowych, planowanie ciągłości działania oraz wyznaczenie osoby odpowiedzialnej za cyberbezpieczeństwo. Część zabezpieczeń technicznych może być wdrażana stopniowo, według udokumentowanego planu uwzględniającego ryzyko i możliwości finansowe jednostki. Nie uchyla to obowiązku wdrożenia podstawowych środków organizacyjnych[47].

5. Realizacja obowiązków cyberbezpieczeństwa w małych gminach – bariery i wyzwania

Przedstawione w rozdziale 4 obowiązki pokazują, że nowy model cyberbezpieczeństwa wymaga od jednostek samorządu terytorialnego nie tylko wdrożenia określonych rozwiązań technicznych, lecz przede wszystkim stworzenia trwałego systemu zarządzania bezpieczeństwem informacji. Pomimo ustawowego zróżnicowania wymagań wobec podmiotów kluczowych i publicznych podmiotów ważnych możliwości realizacji obowiązków są silnie uzależnione od potencjału kadrowego, organizacyjnego i finansowego poszczególnych jednostek. Ten sam obowiązek prawny może stanowić zupełnie inne obciążenie organizacyjne dla dużego miasta dysponującego wyspecjalizowanymi komórkami IT i cyberbezpieczeństwa oraz dla niewielkiej gminy posiadającej ograniczone zasoby kadrowe i finansowe.

Szczególnym wyzwaniem dla małych jednostek może być zapewnienie ciągłego charakteru procesu zarządzania ryzykiem. Realizacja tego zadania wymaga nie tylko opracowania dokumentacji, lecz także jej regularnego przeglądu, monitorowania zagrożeń i aktualizowania zastosowanych środków bezpieczeństwa. Przy ograniczonych zasobach kadrowych powstaje ryzyko sprowadzenia systemu zarządzania bezpieczeństwem informacji do formalnego opracowania wymaganej dokumentacji, bez zapewnienia jego rzeczywistego funkcjonowania w codziennej działalności urzędu.

Zapewnienie bezpieczeństwa łańcucha dostaw może być szczególnie problematyczne w przypadku gmin, które w znacznym stopniu korzystają z usług zewnętrznych dostawców IT. Ograniczony potencjał kadrowy utrudnia samodzielną ocenę poziomu bezpieczeństwa wykonawców, weryfikację stosowanych przez nich zabezpieczeń oraz bieżący nadzór nad realizacją usług. Jednocześnie należy pamiętać, że powierzenie obsługi informatycznej podmiotowi zewnętrznemu nie zwalnia kierownictwa gminy z odpowiedzialności za realizację obowiązków ustawowych.

Istotnym wyzwaniem organizacyjnym może być również prawidłowa obsługa i terminowe zgłaszanie incydentów. Krótkie terminy ustawowe wymagają zapewnienia zdolności do wykrycia zdarzenia, jego wstępnej oceny i klasyfikacji oraz przekazania wymaganych informacji właściwemu CSIRT-owi. W małej gminie szczególnego znaczenia nabiera

[47] Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB), Kybernetická bezpečnost obcí, wersja 1.1, 5 stycznia 2026 r., s. 8–10, https://portal.nukib.gov.cz/informacni-servis/podpurne-materialy/67aca68381589befac075202.

wcześniejsze określenie procedury postępowania, podziału odpowiedzialności oraz sposobu komunikacji na wypadek wystąpienia incydentu.

Kolejnym obszarem, w którym szczególnie widoczna jest różnica pomiędzy obowiązkami prawnymi a możliwościami organizacyjnymi małych gmin, jest zapewnienie ciągłości działania. Realizacja tego zadania wymaga przede wszystkim identyfikacji procesów i systemów kluczowych dla realizacji zadań publicznych, określenia sposobu postępowania na wypadek ich niedostępności, zapewnienia możliwości odtworzenia danych i systemów oraz regularnego testowania i aktualizowania przyjętych procedur. W przypadku małych gmin realizacja tych zadań może stanowić istotne wyzwanie organizacyjne. Ograniczone zasoby kadrowe powodują, że te same osoby odpowiadają często zarówno za bieżące utrzymanie systemów teleinformatycznych, jak i za przygotowanie rozwiązań zapewniających ich funkcjonowanie w sytuacjach awaryjnych.

Szczególnego znaczenia nabiera również uzależnienie od zewnętrznych dostawców usług IT. Gmina powinna bowiem posiadać zdolność do kontynuowania najważniejszych procesów również w przypadku niedostępności systemu lub usług świadczonych przez podmiot zewnętrzny. Problem ten ma bezpośrednie przełożenie na zdolność gminy do realizacji zadań publicznych. Niedostępność systemów dziedzinowych, elektronicznego obiegu dokumentów czy systemów wykorzystywanych do komunikacji z mieszkańcami może prowadzić do czasowego ograniczenia możliwości świadczenia usług publicznych. Z tego względu budowanie ciągłości działania powinno obejmować nie tylko rozwiązania techniczne, takie jak wykonywanie kopii zapasowych i zapewnienie możliwości odtworzenia z nich danych, ale również rozwiązania organizacyjne określające sposób funkcjonowania urzędu w okresie niedostępności podstawowych systemów teleinformatycznych.

Istotnym wyzwaniem jest również zmiana roli kierownictwa w systemie cyberbezpieczeństwa. Nowy model regulacyjny odchodzi od traktowania cyberbezpieczeństwa jako zagadnienia pozostającego wyłącznie w kompetencji pracowników odpowiedzialnych za obsługę informatyczną. Kierownik podmiotu uczestniczy w procesie zarządzania cyberbezpieczeństwem, podejmuje decyzje dotyczące systemu zarządzania bezpieczeństwem informacji oraz odpowiada za zapewnienie odpowiednich zasobów organizacyjnych i finansowych. Powierzenie bieżącej obsługi informatycznej pracownikowi urzędu albo zewnętrznemu wykonawcy nie oznacza zatem przeniesienia na te podmioty odpowiedzialności spoczywającej na kierownictwie jednostki.

W przypadku małych gmin to wójt lub burmistrz musi podejmować decyzje dotyczące obszaru wymagającego coraz bardziej specjalistycznej wiedzy. Dotyczy to między innymi akceptowania poziomu ryzyka, zapewnienia środków finansowych na zabezpieczenia, ustalania zakresu odpowiedzialności pracowników oraz nadzorowania realizacji obowiązków wynikających z ustawy. Kierownik jednostki nie musi posiadać wiedzy technicznej właściwej dla specjalisty z zakresu cyberbezpieczeństwa, powinien jednak dysponować wiedzą pozwalającą zrozumieć występujące ryzyka, ocenić ich znaczenie dla funkcjonowania gminy oraz podejmować świadome decyzje zarządcze. W tym kontekście szczególnego znaczenia nabiera wprowadzony przez ustawodawcę obowiązek regularnego szkolenia kierownictwa.

6. Podsumowanie

Przeprowadzona analiza prowadzi do wniosku, że nowe regulacje wynikające z implementacji dyrektywy NIS2 do ustawy o krajowym systemie cyberbezpieczeństwa stanowią istotny krok w kierunku budowy jednolitego systemu cyberbezpieczeństwa administracji publicznej. Przyjęte regulacje czynią cyberbezpieczeństwo jednym z podstawowych elementów codziennego zarządzania podmiotem.

Nowe regulacje różnicują część obowiązków, zachowując ich wspólny rdzeń, podczas gdy potencjał organizacyjny jednostek samorządu terytorialnego jest silnie zróżnicowany. Szczególnie jest to widoczne w przypadku małych gmin, które przy ograniczonych zasobach kadrowych, finansowych i organizacyjnych mogą mieć poważne trudności z prawidłowym i terminowym wywiązaniem się z obowiązków. Stwarza to ryzyko sprowadzenia wdrożenia do tworzenia fasadowej zgodności z przepisami prawnymi, a nie rzeczywistego budowania odporności organizacji. Prawidłowa budowa cyberodporności administracji publicznej wymaga nie tylko odpowiednich regulacji prawnych, ale przede wszystkim trwałego wsparcia organizacyjnego, finansowego i eksperckiego. Połączenie tych elementów może zapewnić rzeczywistą odporność małych gmin na zagrożenia występujące w cyberprzestrzeni.

Jednym z podstawowych kierunków działań powinno być rozwijanie mechanizmów współdzielenia zasobów i kompetencji pomiędzy jednostkami samorządu terytorialnego. Pozytywnie należy w tym kontekście ocenić działania na rzecz utworzenia Lokalnych Centrów Cyberbezpieczeństwa, które mogą stanowić odpowiedź na problem niedoboru specjalistów oraz umożliwić wspólne korzystanie z kompetencji, narzędzi i usług, których samodzielne zapewnienie przez niewielką gminę byłoby trudne organizacyjnie lub nadmiernie kosztowne. Mechanizmy tego rodzaju powinny mieć charakter trwały i systemowy, ponieważ cyberbezpieczeństwo jest procesem ciągłym, a nie zadaniem możliwym do zrealizowania w ramach jednorazowego projektu.

Istotnym kierunkiem działań powinno być również zapewnienie małym gminom trwałego wsparcia eksperckiego, w szczególności w zakresie zarządzania ryzykiem, oceny bezpieczeństwa łańcucha dostaw, reagowania na incydenty oraz zapewnienia ciągłości działania. Wsparcie takie mogłoby obejmować opracowywanie wzorcowych procedur, metodyk i dobrych praktyk dostosowanych do specyfiki małych jednostek samorządu terytorialnego. Pozwoliłoby to ograniczyć ryzyko przeznaczania znacznej części ograniczonych zasobów na formalne przygotowanie dokumentacji zamiast na rzeczywiste podnoszenie poziomu cyberbezpieczeństwa.

Uwzględniając już istniejące zróżnicowanie wymagań, w perspektywie *de lege ferenda* warto rozważyć szersze wykorzystanie zasady proporcjonalności przy określaniu sposobu realizacji obowiązków w zakresie cyberbezpieczeństwa. Punktem odniesienia powinien być nie tylko rodzaj podmiotu, lecz również skala jego działalności, charakter wykorzystywanych systemów, zakres świadczonych usług oraz rzeczywisty poziom ryzyka. Inspiracji w tym zakresie może dostarczać przedstawiony w artykule model czeski. Zasada proporcjonalności nie powinna oznaczać rezygnacji z podstawowych wymagań bezpieczeństwa ani obniżenia poziomu ochrony mieszkańców małych gmin, lecz umożliwiać dostosowanie sposobu realizacji obowiązków do rzeczywistego ryzyka i możliwości organizacyjnych jednostki.

Ostatecznie skuteczność nowych regulacji powinna być oceniana nie tylko przez stopień formalnego wykonania obowiązków ustawowych, lecz przede wszystkim przez rzeczywistą zdolność jednostki do zapobiegania incydentom, reagowania na nie oraz utrzymania lub szybkiego odtworzenia kluczowych usług publicznych.

Bibliografia

Literatura, raporty i materiały internetowe

- Banasiński C., Rojszczak M., Chmielewski J.M., Hydzik W., Łuczak J., Nowak W., Waćkowski K., Krajowy system cyberbezpieczeństwa [w:] Cyberbezpieczeństwo, Warszawa 2020.
- Bujalski R., Nowe środki w zakresie cyberbezpieczeństwa (dyrektywa NIS2), LEX/el. 2023.
- Centrum Projektów Polska Cyfrowa, Cyberbezpieczny Samorząd, https://www.gov.pl/web/cppc/cyberbezpieczny-samorzad.
- Centrum Projektów Polska Cyfrowa, Działanie 4.1 – Cyberbezpieczeństwo, trzeci nabór, FERC.04.01-IP.01-003/26 (Lokalne Centra Cyberbezpieczeństwa), 2026, https://www.gov.pl/web/cppc/FERC0401IP0100326.
- CERT Polska, Krajobraz bezpieczeństwa polskiego internetu. Raport roczny 2023 z działalności CERT Polska, https://cert.pl/uploads/docs/Raport_CP_2023.pdf.
- CERT Polska, Krajobraz bezpieczeństwa polskiego internetu. Raport roczny 2024 z działalności CERT Polska, https://cert.pl/uploads/docs/Raport_CP_2024.pdf.
- CERT Polska, Krajobraz bezpieczeństwa polskiego internetu. Raport roczny 2025 z działalności CERT Polska, https://cert.pl/uploads/docs/Raport_CP_2025.pdf.
- Czaplicki K., Zapewnienie pożądanego poziomu cyberbezpieczeństwa procesów informacyjnych realizowanych w małych i średnich gminach [w:] Cyberbezpieczeństwo – współpraca vs. konfrontacja informacyjna. Prawo – Informatyka – Zarządzanie, red. B. Szafrański, Warszawa 2025, s. 73–82.
- Drożdżewicz P., Grudzińska E., Hołubowicz K., Pawluczuk A., Strony internetowe urzędów gmin jako element wsparcia e-administracji w gminie, „Samorząd Terytorialny" 2014, nr 5, s. 36–47.
- Dyrektywa NIS2. Komentarz, red. M. Jakubik, R.T. Prabucki, Gdańsk 2026.
- Dziomdziora W.Z., Cyberbezpieczeństwo w samorządzie terytorialnym. Praktyczny przewodnik, Warszawa 2021.
- Edtech Hub Accelerator, Preferencje jednostek samorządu terytorialnego w zakresie wdrożenia nowych innowacji i e-usług, 2020.
- Górnisiewicz M., Skuteczne zarządzanie ciągłością działania [w:] Zarządzanie ryzykiem bankowym, red. M. Iwanicz-Drozdowska, Warszawa 2024.
- Gryszczyńska A., Cyberbezpieczeństwo w jednostkach samorządu terytorialnego [w:] System Prawa Samorządu Terytorialnego, t. III, Samodzielność samorządu terytorialnego – granice i perspektywy, red. I. Lipowicz, Warszawa 2023.
- Gryszczyńska A., Postulaty zmian w zakresie jawności i bezpieczeństwa rejestrów publicznych [w:] Jawność i jej ograniczenia, red. G. Szpor, t. XII, Model regulacji, red. T. Bąkowski, Warszawa 2016, s. 181–197.
- Internet. Hacking, red. A. Gryszczyńska, G. Szpor, W.R. Wiewiórowski, Warszawa 2023.

- ISO 22301:2019, Security and resilience – Business continuity management systems – Requirements.
- Jawność i jej ograniczenia, t. I, Idee i pojęcia, red. G. Szpor, C.H. Beck, Warszawa 2017.
- Kańduła S., W stronę elektronicznej administracji w gminach, „Finanse Komunalne" 2023, nr 2, s. 7–26.
- Kasprzyk B., Aspekty funkcjonowania e-administracji dla jakości życia obywateli, „Nierówności Społeczne a Wzrost Gospodarczy" 2011, nr 23, s. 343–353.
- Kępa L., Bezpieczeństwo danych osobowych. Podejście oparte na ryzyku, C.H. Beck, Warszawa 2019, Legalis.
- Komisja Europejska, eGovernment Benchmark 2024, https://digital-strategy.ec.europa.eu/en/library/digital-decade-2024-egovernment-benchmark.
- Lipowicz I., Odporność samorządu terytorialnego, „Samorząd Terytorialny" 2025, nr 4, s. 32–42.
- Ministerstwo Cyfryzacji, Cyberbezpieczny Samorząd – zakończenie naboru, https://www.gov.pl/web/baza-wiedzy/cyberbezpieczny-samorzad--zakonczenie-naboru.
- Ministerstwo Cyfryzacji, Kluczowe wnioski z raportu eGovernment Benchmark 2024, 19 lipca 2024 r., https://www.gov.pl/web/cyfryzacja/kluczowe-wnioski-z-raportu-egovernment-bench-2024mark-2024.
- Ministerstwo Cyfryzacji, Nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa (KSC) – obowiązki podmiotów kluczowych i ważnych, https://www.gov.pl/web/cyfryzacja/nowelizacja-ustawy-o-krajowym-systemie-cyberbezpieczenstwa-ksc---obowiazki-podmiotow-kluczowych-i-waznych.
- Ministerstwo Cyfryzacji, Węzeł Krajowy – zintegrowani dostawcy usług, https://archiwum_mc.bip.gov.pl/wezel-krajowy-zintegrowani-dostawcy-uslug/wezel-krajowy-zintegrowani-dostawcy-uslg.html.
- Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB), Kybernetická bezpečnost obcí, wersja 1.1, 5 stycznia 2026 r., https://portal.nukib.gov.cz/informacni-servis/podpurne-materialy/67aca68381589befac075202.
- National Institute of Standards and Technology (NIST), Developing Cyber-Resilient Systems: A Systems Security Engineering Approach, NIST SP 800-160, vol. 2, rev. 1, 2021, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2r1.pdf.
- Portal Samorządowy, Cyberbezpieczeństwem wójt się nie pochwali. Ale małe gminy zaczynają się budzić, relacja z CYBERSEC EXPO & FORUM 2026, https://www.portalsamorzadowy.pl/smart-city/cyberbezpieczenstwem-wojt-sie-nie-pochwali-ale-male-gminy-zaczynaja-sie-budzic,665039.html.
- Silicki K., Cyberodporność wspierana przepisami prawa UE: akt o cyberodporności (CRA) i dyrektywa NIS2 [w:] Internet. Cyberodporność, red. A. Gryszczyńska, G. Szpor, W.R. Wiewiórowski, Warszawa 2025, s. 105–117.
- Skoczylas D., Cyberzagrożenia w cyberprzestrzeni. Cyberprzestępczość, cyberterroryzm i incydenty sieciowe, „Prawo w Działaniu" 2023, nr 53, s. 97–113.

- Skoczylas D., Wzmocnienie zdolności Unii Europejskiej w zakresie cyberbezpieczeństwa – cybersolidarność w kontekście cyberzagrożeń, „Europejski Przegląd Sądowy" 2024, nr 12, s. 39–44.
- Szpor G. [w:] Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz, red. K. Czaplicki, A. Gryszczyńska, G. Szpor, Warszawa 2019.
- Szpor G., The Concept of Cyber Resilience in the European Union Law, „Review of European and Comparative Law" 2026, t. 64, nr 1, s. 103–116.
- Szpor G., The Evolution of Cybersecurity Regulation in the European Union Law and Its Implementation in Poland, „Review of European and Comparative Law" 2021, nr 3.
- Tubek B., E-administracja i jej wpływ na współczesne społeczeństwo informacyjne, „Roczniki Administracji i Prawa" 2025, nr 2, s. 125–139.
- W drodze ku doskonałości cyfrowej. Raport końcowy z badania rynku na temat gotowości wdrożenia, poziomu wiedzy i wykorzystania nowych technologii cyfrowych w jednostkach samorządu terytorialnego, Warszawa 2023.
- Woszek S., Cyberbezpieczeństwo państw w XXI wieku na przykładzie Rzeczypospolitej Polskiej, „Przegląd Bezpieczeństwa Wewnętrznego" 2022, nr 27(14).

Akty prawne

- Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS2) (Dz. Urz. UE L 333 z 27.12.2022, s. 80, z późn. zm.).
- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 4.05.2016, s. 1 z późn. zm.).
- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie) (Dz. Urz. UE L 151 z 7.06.2019, s. 15 z późn. zm.).
- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011 (Dz. Urz. UE L 333 z 27.12.2022, s. 1, z późn. zm.).
- Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (Dz. Urz. UE L 257 z 28.08.2014, s. 73 z późn. zm.).

- Rozporządzenie Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2024 r. poz. 773).
- Uchwała nr 92 Rady Ministrów z dnia 10 marca 2026 r. w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej (M.P. poz. 309).
- Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz. U. z 2025 r. poz. 1703 z późn. zm.).
- Ustawa z dnia 23 stycznia 2026 r. o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (Dz. U. poz. 252).
- Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (t.j. Dz. U. z 2026 r. poz. 574 z późn. zm.).
- Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2026 r. poz. 20 z późn. zm.).
- Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (t.j. Dz. U. z 2024 r. poz. 1725 z późn. zm.).

O AUTORZE

dr Kamil Czaplicki

Doktor nauk prawnych, pracownik Katedry Prawa Informatycznego na Wydziale Prawa i Administracji Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie. Autor publikacji dotyczących cyberbezpieczeństwa, ochrony danych osobowych i identyfikacji tożsamości. Współredaktor komentarza do ustawy o krajowym systemie cyberbezpieczeństwa.

Źródło noty: UKSW, Katedra Prawa Informatycznego, https://kpi.uksw.edu.pl/node/65.

STRESZCZENIE

Analiza przedstawia wpływ dyrektywy NIS2 i nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa na małe gminy. Jej celem jest ocena relacji między obowiązkami prawnymi a zasobami kadrowymi, organizacyjnymi i finansowymi samorządów. Autor wskazuje, że formalna zgodność z przepisami nie wystarcza do zapewnienia cyberodporności. Rekomenduje współdzielenie zasobów, rozwój Lokalnych Centrów Cyberbezpieczeństwa, trwałe wsparcie eksperckie i proporcjonalność wymagań.

Słowa kluczowe

cyberbezpieczeństwo, cyberodporność, małe gminy, NIS2, krajowy system cyberbezpieczeństwa

Stan prawny: 24 września 2026 r.

...

Warszawa, wrzesień 2026
Fundacja Rozwoju Demokracji Lokalnej im. Jerzego Regulskiego
ul. Edwarda Jelinka 6, 01-646 Warszawa
WWW.FRDL.ORG.PL